IN THE MATTER OF
KOREAN PATENT APPLICATION
UNDER SERIAL NO. 72949/2000

I, THE UNDERSIGNED, HEREBY DECLARE :
THAT I AM CONVERSANT WITH BOTH THE KOREAN AND THE ENGLISH LANGUAGES : AND

THAT I AM A COMPETENT TRANSLATOR OF THE APPLICATION PAPERS THE PARTICULARS OF WHICH ARE SET FORTH BELOW :

KOREAN PATENT APPLICATION UNDER SERIAL NO.:	72949/2000
FILED ON :	DECEMBER 4, 2000
IN THE NAME OF :	LG ELECTRONICS INC.
FOR :	INTERNET ACCESS METHOD USING AN INTENET TV

IN WITNESS WHEREOF, I SET MY HAND HERETO

THIS 22TH DAY OF JUNE, 2006

BY Han

Ji Eun, HAN

[Translation]

PATENT APPLICATION

Name of Document	: Patent Application
Classification of Right	: Patent
Receiver	: Commissioner of the Patent Office
Application Number	: 09/996,718
Filing Date	: December 4, 2000
Int'l Classification	: H04N
Title of the Invention	: Internet Access Method Using an Internet TV
Applicant	: Name : LG ELECTRONICS INC. Code No. : 1-1998-000275-8
Attorney	: Name : Yong Rok HUR Code No.: 9-1998-000616-9 Reg. No. of General Authorization: 1999-043458-0
Inventors	: Name : YU, Won Uk Resident Reg. No.: 640126-1691629 Zip code : 702-280 Address: Geumbittaun Apt.102-1307, 655 Guam-Dong, Buk-Gu, Daegu, Korea Nationality : Korean

This application is hereby filed pursuant to Article 42 of the Patent Law.

/S/ Attorney : Yong Rok HUR

[Translation]

ABSTRACT OF THE DISCLOSURE

[Abstract]

A method for accessing the Internet using an Internet TV according to the present invention comprises the steps of: connecting the Internet TV with an Internet portal site through a network and transmitting an authentication request signal regarding the use of information; requesting the Internet TV to input an authentication number by the Internet portal site; transmitting the requested authentication number to the Internet portal site by the Internet TV; and checking the authentication number transmitted from the Internet TV by the Internet portal site, to thus provide information to the Internet TV when the authentication number is judged as the Internet TV allowing the access.

Further, another embodiment of the Internet access method using the Internet TV in accordance with the present invention comprises the steps of: connecting the Internet TV with an Internet portal site through a network and transmitting an authentication request signal regarding the use of information; requesting the Internet TV to input an authentication number from the Internet portal site; judging whether the present proceeding state is an initialization state or not at the Internet TV; transmitting a message for requesting the authentication number search to the Internet portal site at Internet TV when the present state is a state for proceeding the initialization; inputting the user's information requested from the Internet portal site at Internet TV; and receiving the authentication number transmitted from the Internet portal site at the Internet TV and storing the received authentication number to the memory.

[Representative drawing]

Figure 2

[SPECIFICATION]

[Title of the Invention]

INTERNET ACCESS METHOD USING AN INTERNET TV

[Brief description of the Drawings]

Figure 1 is a block diagram roughly showing a construction of a general Internet TV.

Figure 2 is a drawing showing a signal flow between the Internet TV and an Internet portal site by the Internet access method using the Internet TV according to the present invention.

Figure 3 is a flowchart showing the operation of the Internet TV for accessing the Internet portal site according to the present invention.

Figure 4 is a flowchart showing the operation regarding the Internet TV connection in the Internet portal site according to the present invention.

Figure 5 is a drawing showing an example of an user information input screen according to the present invention.

Figure 6 is a drawing showing an example of a generating method and a checking method of the authentication number according to the present invention.

**** Explanation for the major reference numerals ****

100: Internet TV 101: RAM

102: hard disk 103: audio signal output unit

104: radio input device interface unit 105: control unit

106: audio signal processing unit 107: video signal output unit

108: video signal processing unit 109: network interface unit

[Detailed description of the invention]

[Object of the invention]

[Field of the invention and background art]

The present invention relates to a method for accessing the Internet using an Internet TV, and more particularly, to a method for accessing the Internet using an Internet TV, in which an authentication number is provided to each Internet TV by an Internet portal site, to thus check the accessing right of each Internet TV at the Internet portal site and manage the use of information by the user.

Recently, the efficiency of works epochally improves and life-styles largely change due to the rapid growth of information communication field relevant to computers. For instance, the use of product purchasing method using online shopping mall on the network in the shopping style relevant to the product purchasing is gradually being extended.

Further, a network having data access speed of several Mbit/sec is installed at home with rapid spread of a very high-speed communication network. Accordingly, it is possible to use moving picture information of high picture quality and high performance at home.

Meanwhile, the development regarding the Internet terminal connectable to the Internet and the protocol for operating the mobile communication system is actively being progressed by using the mobile communication terminal together with the propagation of the mobile communication terminal.

Further, the development regarding the Internet TV combining a function of accessing the Internet and a function of receiving TV broadcast is also actively being proceeded. The Internet TV that is a next generation TV, in which modem is loaded, can freely access the Internet as well as can perform a common TV function. The Internet TV is divided into an armored type connected to a personal computer and a built-in type, in which Internet receiving board, software and modem are installed within TV receiver. The technology of the built-in Internet TV is more difficult than the technology of the armored Internet TV. However, the picture quality of the built-in type Internet TV is excellent and the manipulation of the built-in type Internet TV is convenient since RGB input terminals can be used as they are.

As described in the above, the development regarding the Internet access using TV by means of Internet settop box is actively being proceeded.

[Technical solution to be achieved by the invention]

The present invention has been invented by considering the above-mentioned conditions. Therefore, an object of the present invention is to provide an Internet access method using the Internet TV capable of checking access right of each Internet TV by the Internet portal site and managing the use of the user information by giving the authentication number to each Internet TV in the Internet portal site.

[Construction of the invention]

The Internet access method using the Internet TV according to the present invention for obtaining the above-mentioned objects, comprising the steps of:

connecting the Internet TV with an Internet portal site through a network and transmitting an authentication request signal regarding the use of information;

requesting the Internet TV to input an authentication number by the Internet portal site;

transmitting the requested authentication number to the Internet portal site by the Internet TV; and

checking the authentication number transmitted from said Internet TV by said Internet portal site, to thus provide information to said Internet TV when the authentication number is judged as the Internet TV allowing the connection.

Further, another embodiment of the Internet access method using the Internet TV according to the present invention comprise the steps of:

(a) connecting the Internet TV with an Internet portal site through a network and transmitting a signal for requesting the authentication of the use of information;

(b) being requested to input an authentication number from the portal site by the Internet TV;

(c) judging whether the present proceeding state is an initialization state or not by the Internet TV;

(d) transmitting an authentication number search request message to the Internet portal site by the Internet TV when the present state is a state for proceeding the initialization;

(e) inputting the user information requested from said Internet portal site by the Internet TV; and

(f) receiving the authentication number transmitted from said Internet portal site and storing the received authentication number to the memory by the Internet TV.

Here, when the present proceeding state is not an initialization state as a result of judging in said step (c), said Internet TV comprises the steps of:

(i) judging whether the allocated authentication number exists or not;

(j) transmitting the authentication number to said Internet portal site when there is an allocated authentication number; and

(k) receiving the information from said Internet portal site when a normal authentication number is submitted as a result of checking the authentication number transmitted from said Internet portal site.

Further, when there exists not allocated authentication number as a result of the judgement in said step (i), said Internet TV comprises the steps of:

transmitting a message for newly requesting the authentication number regarding the use of the information to said Internet portal site;

performing the user registration according to the user registration form requested from said Internet portal site; and

receiving the new authentication number provided from said Internet portal site and storing the received authentication number in the memory.

Further, another embodiment of the Internet access method using the Internet TV according to the present invention for obtaining said objects is characterized by the Internet portal site, comprising the steps of:

(o) receiving the authentication request message regarding the use of the information from the Internet TV through the network;

(p) requesting to input the authentication number allocated to said Internet TV;

(q) judging whether the inputted message is a request message for the authentication number search by the message inputted from said Internet TV;

(r) transmitting the message requesting to input the user information to said Internet TV when the message received from said Internet TV is a message requesting the authentication number search as a result of the judging in said step (q);

(s) judging whether the user is registered to the user database with reference to the

user information transmitted from said Internet TV; and

(t) transmitting to said Internet TV by obtaining the authentication number when the information regarding said Internet TV user is registered in the data base.

Here, when the message received from said Internet TV is not a message requesting the authentication number search as a result of judging in said step (q), said Internet portal site comprises the steps of:

(v) judging whether the message transmitted from said Internet TV provides the information regarding the allocated authentication number;

(w) judging whether there exists an error by reading the received authentication number when the authentication number allocated from said Internet TV is transmitted as a result of the judgement in said step (v);

(x) providing the information by considering with the user information registered in the database when there exists no error in the authentication number transmitted from said Internet TV as a result of the judgement in said step (w).

Further, said Internet portal site comprises the steps of: obtaining the information on the payment of fee of the user in consideration of the user information registered in the database when there exists no error in the authentication number transmitted from said Internet TV in said step (x); and transmitting the message of noticing the unpaid fee to said Internet TV when there exists unpaid fee.

Further, when the authentication number allocated from said Internet TV is not transmitted as a result of judging in said step (v), said Internet portal site comprises the steps of:

judging whether the message for newly requesting the authentication number is transmitted from said Internet TV;

transmitting the user registration request message to said Internet TV when the

message for newly requesting the authentication number is received from said Internet TV; and

when the user registration is performed from said Internet TV user, allocating the authentication number to said Internet TV and transmitting the allocated authentication number to said Internet TV.

In accordance with the present invention, there are advantages of checking the access right of each Internet TV and managing the use of the user information by the Internet portal site by giving the authentication number to each Internet TV at the Internet portal site.

Hereinafter, the embodiment in accordance with the present invention will be described in detail with reference to the attached drawings.

Figure 1 is a block diagram roughly showing a construction of a general Internet TV.

Referring to Figure 1, the general Internet TV 100 includes a RAM 101 installing the operation program during the initialization, a hard disk 102 recording software and data necessary for the operation, radio input device interface unit 104 inputting the command from outer radio input device such as a wireless keyboard, a wireless mouse and a remote control, an audio signal processing unit 106 processing the audio signal, an audio signal output unit 103 such as a speaker outputting the audio signal processed at said audio signal processing unit 106 to the outside, a video signal processing unit 108 processing the video signal, a video signal output unit 107 such as a monitor outputting the video signal processed at said vide signal processing unit 108, a network interface unit 109 connecting to the outer network such as the Internet and a control unit 105 controlling said various constitutional elements 101 102 104 106 108 and 109. Further, said network interface unit 109 is connected to the outer network through a cable modem,

a LAN, an ADSL modem, a telephone line modem, etc.

Then, the procedure for connecting to the Internet portal site and being provided the information using the Internet TV having such construction may conceptually be explained by referring to Figure 2. Figure 2 is a drawing showing a signal flow between the Internet TV and the Internet portal site by the Internet access method using the Internet TV according to the present invention.

Referring to Figure 2, first, the Internet TV accesses to the Internet portal site through the network such as the Internet and transmits the authentication request signal. Then, said Internet portal site requests for inputting the authentication number regarding the access allowance to said Internet TV.

According to this, said Internet TV obtains the authentication number being requested to input from said Internet portal site from the data base recorded in the memory such as the hard disk and transmits the obtained authentication number to said Internet portal site. Then, said Internet portal site checks the authentication number transmitted from said Internet TV and provides the information to said Internet TV when the authentication number is judged as the Internet TV allowing the connection.

The process flow in the Internet TV and the process flow in the Internet portal site will now be described in detail with reference to Figures 3 and 4. Figure 3 is a flowchart showing the operation of the Internet TV for accessing the Internet portal site according to the present invention and Figure 4 is a flowchart showing the operation regarding the Internet TV connection in the Internet portal site according to the present invention.

First, explaining the operating procedure in the Internet TV with reference to Figure 3, the Internet TV performs the initialization routine by the operation of the user (Step 301). That is, said Internet TV let the application programs (operation system, browser, etc.) necessary for the Internet access drive.

Then, said Internet TV tries to access the Internet portal site (Step 302) and informs the information that the Internet TV tries to access by transmitting the authentication request signal regarding the access allowance, for instance, a message referred to as TN-100 created by CGI (Step 303).

At this time, said Internet TV examines whether the input of the authentication number allocated to said Internet TV is requested from the Internet portal site trying to access and is in a stand-by state (Step 304).

Further, said Internet TV examines whether the current state of the Internet TV is the initialization procedure when the input of the authentication number allocated to the Internet TV is requested from said Internet portal site in said Step 304 (Step 305). Here, the initialization procedure represents the procedure of automatically being recovered to the state set as default due to the generation of problems in the operation program of said Internet TV.

Meanwhile, said Internet TV requests the search for the authentication number by transmitting the message, for instance, a message referred to as URL_A?Serial=search created by the CGI to the Internet portal site trying to access when the current processing state is the initialization procedure of the Internet TV as a result of the judgement in said Step 305 (Step 306).

According to this, said Internet portal site outputs the screen such as Figure 5 to the Internet TV and requests the input of the user information such as the information of the resident registration number, the name, etc., and the Internet TV user inputs the user information and transmits it to said Internet portal site (Step 307). Here, Figure 5 is a drawing showing the example of the user information input screen in the Internet access method using the Internet TV according to the present invention.

Further, said Internet TV receives the authentication number, for instance, an

authentication number transmitted by a java script method (This authentication number is an information allocated to said Internet TV through the conventional user registration and is a data wherein said Internet portal site searches the database and transmits it.) from said Internet portal site (Step 308) and stores the authentication number received to the hard disk (Step 309).

Meanwhile, said Internet TV judges whether there exists an authentication number necessary for accessing said Internet portal site when the proceeding state of the current Internet TV is not an initialization procedure as a result of the judgement in said Step 305.

At this time, said Internet TV transmits the stored authentication number, for instance, the message referred to as 'URL_A?Serial=XXXXX' created by the CGI to said Internet portal site when there is the authentication number necessary for accessing said Internet portal site as a result of the judgement in said Step 311 (Step 312).

Then, said Internet TV receives the examination result regarding the authentication number replied from the Internet portal site (Step 313). At this time, said Internet TV examines whether there is an 'check sum' error in the examination result regarding the authentication number (Step 314), receives the information from said Internet portal site when there is no 'check sum' error, and displays it on the monitor by decoding (Step 315).

Meanwhile, said Internet TV performs the procedure after said Step 307 which inputs and transmits the user information to said Internet portal site when there is 'check sum' error as a result of the judgement in said Step 314.

Further, said Internet TV requests to issue new authentication number by transmitting the message, for instance, a message referred to as 'URL_A?Serial=new' created by the CGI, to said Internet portal site when the authentication number is not

stored as a result of the judgement in said Step 311 (Step 321).

According to this, said Internet TV user performs the user registration in accordance with the user registration form requested from said Internet portal site (Step 322). Then, said Internet TV user receives the authentication number from said Internet portal site (Step 323) and stores the received authentication number in the memory such as the hard disk (Step 324). Through the above-mentioned procedures, said Internet TV may receive the information from said Internet portal site giving the authentication number and display the information on the monitor.

The procedure of processing the Internet TV access in the Internet portal site will now be explained with reference to Figure 4.

First, the Internet portal site performs a main program together with the operation (Step 401). Then, said Internet portal site judges whether the access request is received through the network and is in the stand-by state (Step 402), and receives the request message when there is an access request through the network (Step 403).

At this time, said Internet portal site judges whether the access request message received in said Step 403 is a message requested from the Internet TV, for instance, the '(TN-100)' message created by the CGI (Step 404). Then, said Internet portal site performs the procedure after said Step 401 when the received message is not a message requested from the Internet TV as a result of the judgement in said Step 404.

Further, said Internet portal site requests to input the authentication number to the corresponding Internet TV when the received message is a message requested from the Internet TV, for instance, '(TN-100)' message created by the CGI as a result of the judgement in said Step 404 (Step 405).

Then, said Internet portal site judges whether the data transmitted from said Internet TV is a message requesting for searching the authentication number, for instance,

'URL_A?Serial=search' message created by the CGI (Step 406).

At this time, said Internet portal site requests to input the user information to said Internet TV when the message transmitted from said Internet TV requests the search for the authentication number as a result of the judgement in said Step 406 (Step 407).

Then, said Internet portal site judges whether the authentication number regarding the corresponding Internet TV exists in the database by referring to the user information transmitted from the Internet TV for the request in said Step 407 (Step 408).

As a result of judging in said step 408, when there exists the authentication number regarding the corresponding Internet TV in the data base, said Internet portal site transmits the authentication number to said Internet TV (Step 409).

Meanwhile, as a result of the judging in said step 406, when the message transmitted from said Internet TV is not a search request regarding the authentication number, said Internet portal site judges whether the form of the received message inputs the authentication number of said Internet TV, for instance, 'URL_A?Serial=XXXXX' message (Step 411).

At this time, said Internet portal site reads the received authentication number when the form of the received message is the authentication number of the Internet TV as a result of the judgement in said Step 411 (Step 412) and examines whether the 'check sum' regarding the received authentication number is correct (Step 413).

Here, the method for checking the 'check sum' of said Internet portal site may be various, and as shown in Figure 6, the 'check sum' may be generated and examined by using the manufacturing date and the model name of the Internet TV. Figure 6 is a drawing showing an example of a generating method and a checking method of the authentication number according to the present invention.

As a result of the examination in said Step 413, when the 'check sum' regarding

the received authentication number is correct, said Internet portal site judges whether the authentication number is user registered in the database (Step 414).

Meanwhile, said Internet portal site judges whether the user fee is normally charged when the user is registered in the database (Step 415) and provides the information to said Internet TV when the fee is normally charged (Step 416).

Then, as a result of the judging in said Step 415, when the fee is not normally charged, said Internet portal site transmits the message for informing the unpaid fee to said Internet TV (Step 417).

Further, said Internet portal site transmits the 'check sum' error message to said Internet TV when the 'check sum' regarding the received authentication number is not correct as a result of the judgement in said Step 413 (Step 418) and performs the procedure after said Step 407 requesting to input the user information.

Meanwhile, said Internet portal site judges whether the message received from said Internet TV is a request to newly issue the authentication number, for instance, 'URL_A?Serial=new' message when the form of the received message is not an input of the authentication number as a result of the judgement in said Step 411 (Step 421).

At this time, when the issue of the authentication number is newly requested as a result of judging in said Step 421, said Internet portal site transmits the user registration screen to said Internet TV (Step 422). Then, said Internet portal site examines whether the user registration is performed from the Internet TV user and is in the stand-by state (Step 423), and when the user registration is performed, the Internet portal site generates the authentication number regarding the corresponding Internet TV and transmits it to said Internet TV (Step 424).

Then, said Internet portal site performs the procedure of said Step 422 for transmitting the user registration screen to said Internet TV again when the user

registration is not normally performed as a result of judging in said Step 243.

Further, when the authentication number issue is not newly requested as a result of the judgement in said Step 421, said Internet portal site performs the procedure after said Step 405 for requesting the authentication number input to the Internet TV trying to access.

Meanwhile, when the corresponding user is not registered in the database as a result of the examination in said Steps 408 and 414, said Internet portal site performs the procedure after said Step 422 for transmitting the user registration screen to the corresponding Internet TV.

[Effect of the invention]

As so far described, according to the Internet access method using the Internet TV of the present invention, the Internet portal site has advantages for checking the access right of each Internet TV and managing the use of the user information by giving the authentication number to each Internet TV.

Further, according to the Internet access method using the Internet TV in accordance with the present invention, there are advantages that the Internet portal site may determine whether the information is provided to the corresponding Internet TV according to the state of the fee payment of the user.

What is claimed is:

1. An Internet access method using the Internet TV according to the present invention for obtaining the above-mentioned objects, comprising the steps of:

connecting the Internet TV with an Internet portal site through a network and transmitting an authentication request signal regarding the use of information;

requesting the Internet TV to input an authentication number by the Internet portal site;

transmitting the requested authentication number to the Internet portal site by the Internet TV; and

checking the authentication number transmitted from said Internet TV by said Internet portal site, to thus provide information to said Internet TV when the authentication number is judged as the Internet TV allowing the connection.

2. The Internet access method using the Internet TV, comprising the steps of:

(a) connecting the Internet TV with an Internet portal site through a network and transmitting a signal for requesting the authentication of the use of information;

(b) being requested to input an authentication number from the portal site by the Internet TV;

(c) judging whether the present proceeding state is an initialization state or not by the Internet TV;

(d) transmitting an authentication number search request message to the Internet portal site by the Internet TV when the present state is a state for proceeding the initialization;

(e) inputting the user information requested from said Internet portal site by the

Internet TV; and

(f) receiving the authentication number transmitted from said Internet portal site and storing the received authentication number to the memory by the Internet TV.

3. The method as claimed in claim 2, when the current proceeding state is not an initialization state as a result of the judgement in said step (c), wherein the Internet TV comprises the steps of:

(i) judging whether the allocated authentication number exists or not;

(j) transmitting the authentication number to said Internet portal site when there is an allocated authentication number; and

(k) receiving the information from said Internet portal site when a normal authentication number is submitted as a result of checking the authentication number transmitted from said Internet portal site.

4. The method as claimed in claim 3, when there exists not allocated authentication number as a result of the judgement in said step (i), wherein said Internet TV comprises the steps of:

transmitting a message for newly requesting the authentication number regarding the use of the information to said Internet portal site;

performing the user registration according to the user registration form requested from said Internet portal site; and

receiving the new authentication number provided from said Internet portal site and storing the received authentication number in the memory.

5. The Internet access method using the Internet TV, comprising the steps of:

(o) receiving the authentication request message regarding the use of the information from the Internet TV through the network;

(p) requesting to input the authentication number allocated to said Internet TV;

(q) judging whether the inputted message is a request message for the authentication number search by the message inputted from said Internet TV;

(r) transmitting the message requesting to input the user information to said Internet TV when the message received from said Internet TV is a message requesting the authentication number search as a result of the judging in said step (q);

(s) judging whether the user is registered to the user database with reference to the user information transmitted from said Internet TV; and

(t) transmitting to said Internet TV by obtaining the authentication number when the information regarding said Internet TV user is registered in the data base.

6. The method as claimed in claim 5, said Internet portal site comprises the steps of:

(v) judging whether the message transmitted from said Internet TV provides the information regarding the allocated authentication number;

(w) judging whether there exists an error by reading the received authentication number when the authentication number allocated from said Internet TV is transmitted as a result of judging in said step (v);

(x) providing the information by considering with the user information registered in the database when there exists no error in the authentication number transmitted from said Internet TV as a result of judging in said step (w).

7. The method as claimed in claim 6, wherein said Internet portal site comprises

the steps of:

obtaining the information on the payment of fee of the user in consideration of the user information registered in the database when there exists no error in the authentication number transmitted from said Internet TV in said step (x); and transmitting the message of noticing the unpaid fee to said Internet TV when there exists unpaid fee.

8. The method as claimed in claim 6, wherein said Internet portal site comprises the steps of:

judging whether the message for newly requesting the authentication number is transmitted from said Internet TV;

transmitting the user registration request message to said Internet TV when the message for newly requesting the authentication number is received from said Internet TV; and

when the user registration is performed from said Internet TV user, allocating the authentication number to said Internet TV and transmitting the allocated authentication number to said Internet TV.

Figure.1

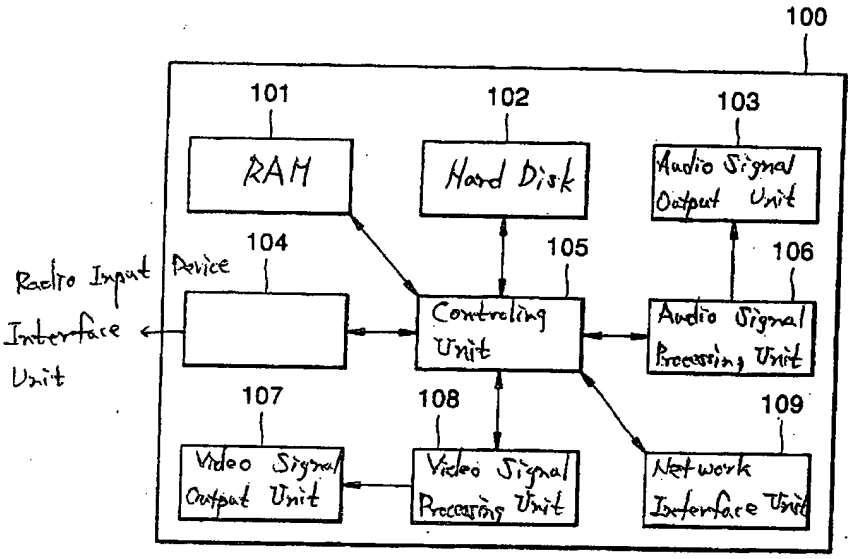


Figure.2

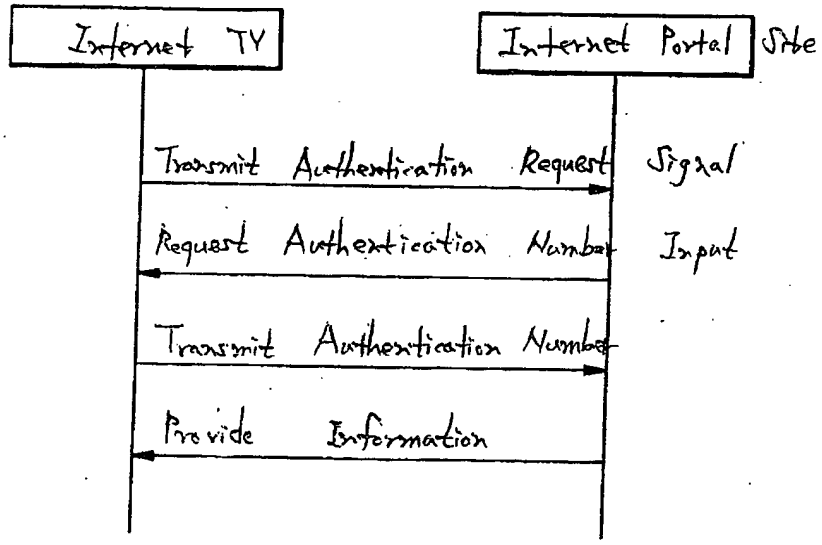
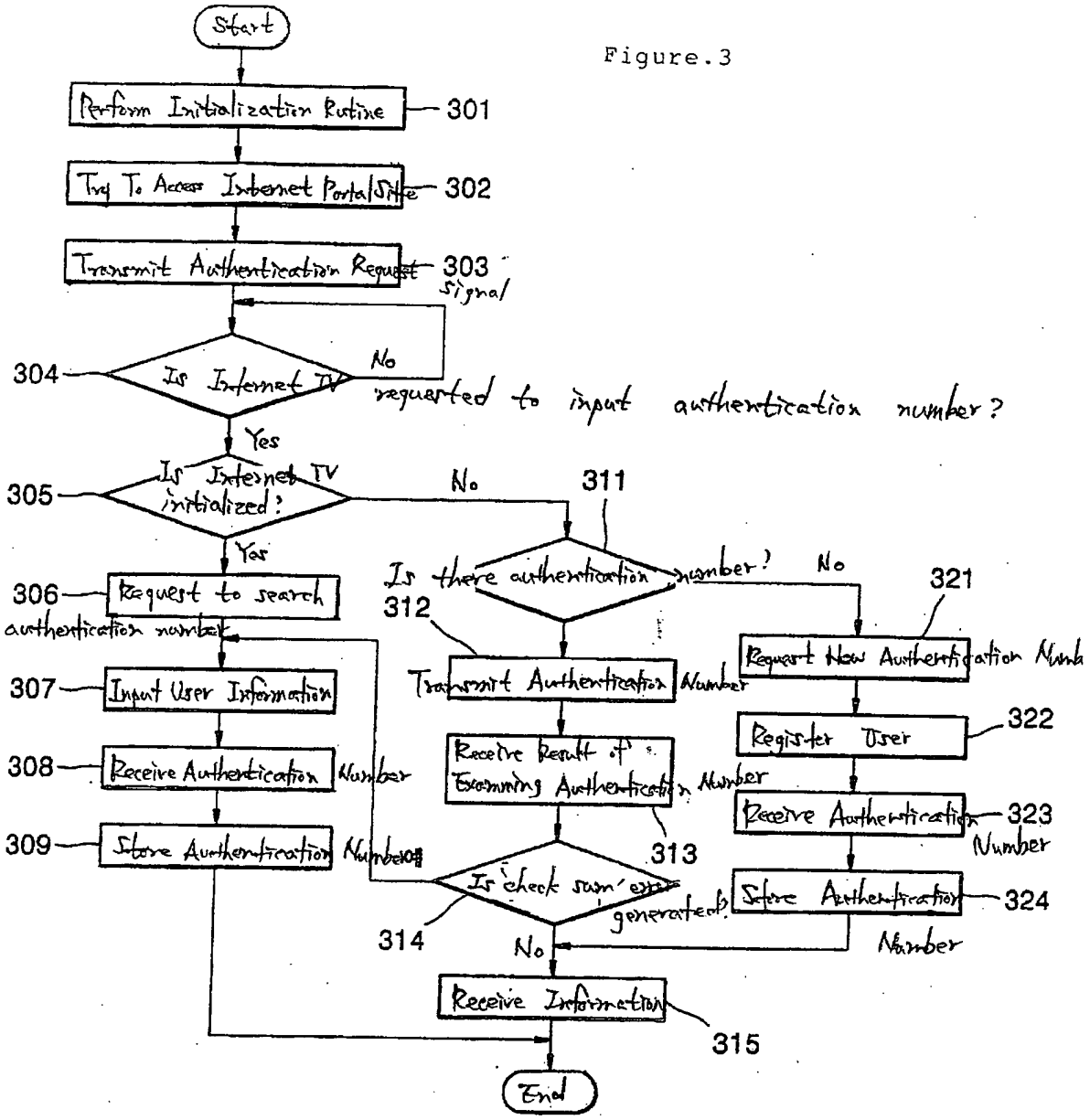


Figure.3


Start
Perform Initialization Routine
301
Try To Access Internet Portal Site
302
Transmit Authentication Request Signal
303
Is Internet TV requested to input authentication number?
304
No
Yes
Is Internet TV initialized?
305
No
311
Yes
Is there authentication number?
No
321
306
Request to search authentication number
312
Request New Authentication Numb
307
Input User Information
Transmit Authentication Number
322
Register User
308
Receive Authentication Number
Receive Result of Examining Authentication Number
323
Receive Authentication Number
309
Store Authentication Number
313
Is check sum error generated?
324
Store Authentication Number
314
No
Receive Information
315
End

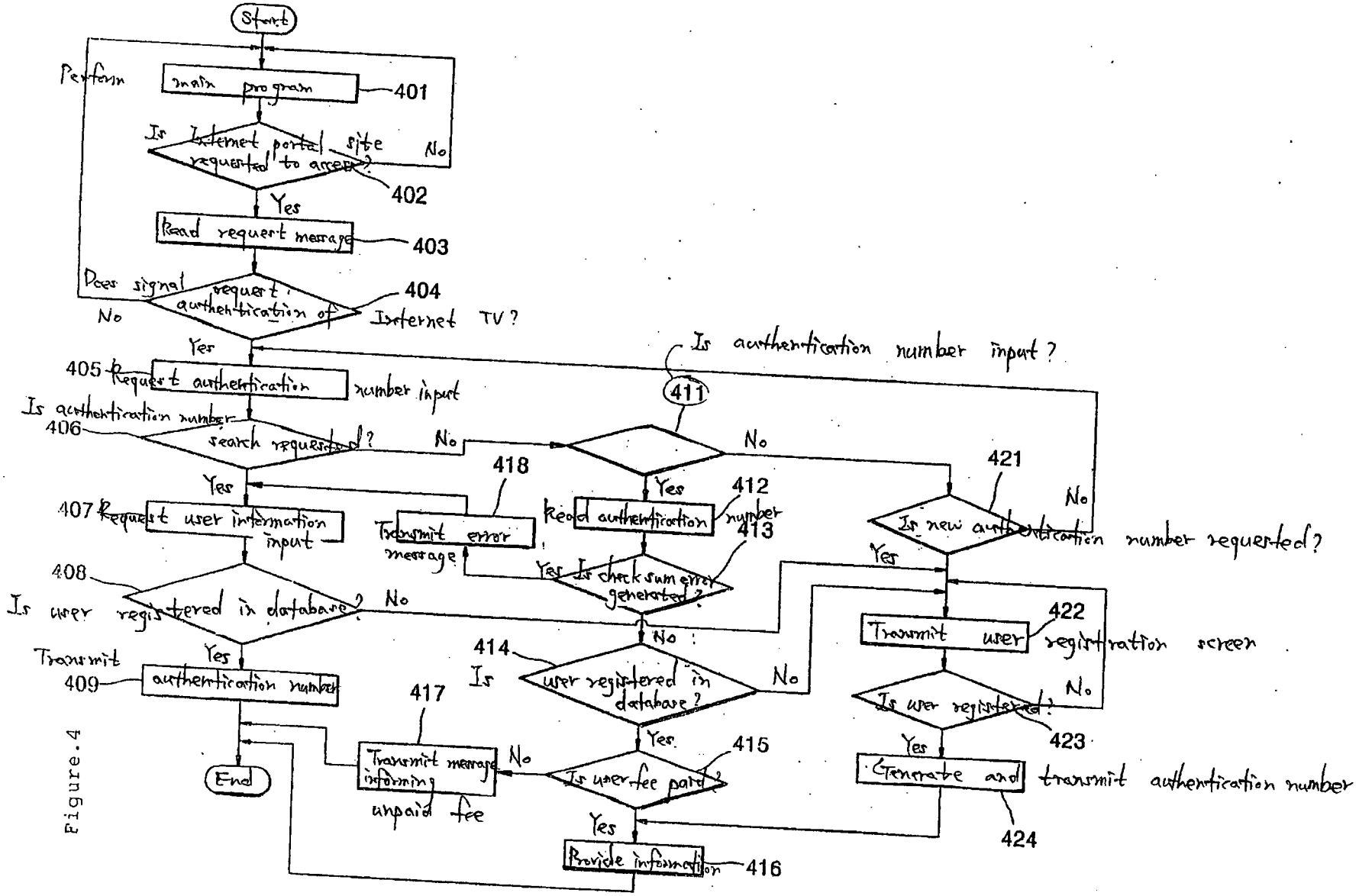

Start
Perform main program
401
Is Internet portal site requested to access?
No
402
Yes
Read request message
403
Does signal request authentication of Internet TV?
404
No
Yes
405 Request authentication number input
Is authentication number search requested?
406
No
Yes
407 Request user information input
408
Is user registered in database?
No
Yes
Transmit authentication number
409
End
Transmit message informing unpaid fee
417
No
Is user fee paid?
415
Yes
Provide information
416
Is user registered in database?
414
No
Yes
Transmit error message
418
Is checksum error generated?
413
Yes
No
Read authentication number
412
Is authentication number input?
411
No
Yes
Is new authentication number requested?
421
No
Yes
Transmit user registration screen
422
Is user registered?
423
No
Yes
Generate and transmit authentication number
424

Figure.4

Figure.5

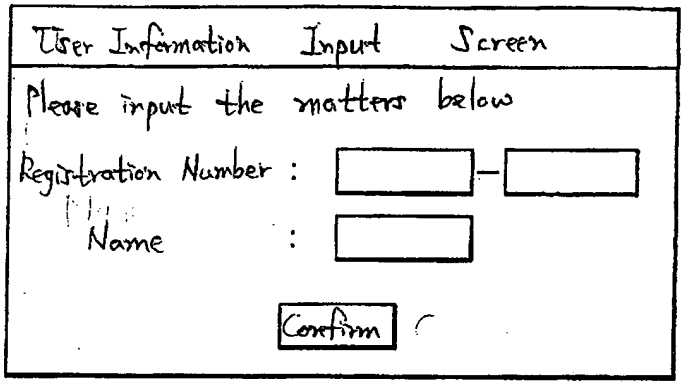


Figure.6

Authentication Number Generation Rule

Model No.	Year	Month	Serial No.	Check Sum
0100	00	11	00001	0

Calculate Check Sum

0	1	0	0	0	0	1	1	0	0	0	0	1
1	2	3	4	5	6	7	8	9	10	11	12	13

2 + 7 + 8 + 13 = 30

30 / 10 의 Remainder → Check Sum

Express Mail mailing label no. EL212282865US
Date of Deposit: March 2, 2000
I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, BOX PROVISIONAL APPLICATION, Washington, D. C. 20231.

By: Vanessa Knowles

Attorney Docket No. TIVO0042PR

IN THE U.S. PATENT AND TRADEMARK OFFICE
Provisional Application Cover Sheet

Assistant Commissioner for Patents
BOX PROVISIONAL APPLICATION
Washington, D.C. 20231

Sir:

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(b)(2).

INVENTOR(s)/APPLICANT(s)

Last Name	First Name	Middle Initial	Residence (City and Either State or Foreign Country
Barton	James	M.	Los Gatos, California
Platt	David		Mountain View, California
Goodman	Andrew		Menlo Park, California
Zenchelsky	Daniel		Los Gatos, California

Additional inventors are being named on separately numbered sheets attached hereto.

Title of the Invention

ENCRYPTION SYSTEM

Correspondence Address

GLENN PATENT GROUP
3475 EDISON WAY, STE. L
MENLO PARK, CA 94025

Telephone No. (650) 474-8400

Enclosed Application Parts *(check all that apply)*

(X) Specification and Drawing(s) *Number of Pages* 13

(X) Small Entity Statement - Business

( ) Other (specify)

Filing Fee and Method of Payment

__X__ $75.00 for Small Entity

_____ $150 for Large Entity

The Commissioner is authorized to charge the filing fee of $150 and any additional fees or credit any overpayment to Deposit Account No. 07-1445 (Order No. TIVO0042PR). A copy is enclosed for this purpose.

Respectfully Submitted,

MICHAEL A. GLENN
Reg. No. 30,176

Provisional Patent Application

Authors: Daniel Zenchelsky, Andy Goodman, David Platt

Background

MPEG is an industry standard for compressing, multiplexing, and transmitting digital video and audio. An MPEG stream is composed of a sequence of data bytes. These bytes can be logically grouped together to form a single element within an MPEG stream. For example, a single element within an MPEG stream might represent a single frame of video within a movie.

The MPEG standard defines byte sequences that indicate the start of an element within an MPEG stream. These byte sequences are referred to as □start codes.□

Some examples of MPEG start codes include: Video Packetized Elementary Stream Header, Video Group Of Pictures Header, Video I Frame Header, Video P Frame Header, Video B Frame Header, Video Slice Header, Audio Packetized Elementary Stream Header.

It is often useful or necessary to build an □Event Table□ that indicates the location of start codes within an MPEG stream. This table is composed of a list of offsets into the MPEG stream. The offsets listed in the table correspond to locations in the MPEG stream that contain start codes.

The Event Table may contain additional information as well. For example, it is often useful to describe what type of start code is located at each offset.

Using the Event Table allows a playback device to quickly locate a particular element within an MPEG stream. For example, one method of quickly scanning through video (□fast forward□) is to play only a subset of the video frames contained within the stream. The Event Table can be used to quickly locate those frames that need to be displayed.

One application where it is useful to build such a table is on a device designed to receive, store, and playback MPEG stream transmissions.

MPEG streams are often encrypted before transmission to prevent unauthorized use. It is often desirable to store the MPEG stream in it□s encrypted form prior to use, in order to prevent unauthorized use.

Typically, the stream is not decrypted until the rights to use the stream are purchased. The Event Table can not be built until the MPEG stream is decrypted. Building the Event Table can be a time consuming process. This can impose a significant time delay between the time that the rights to use the stream are purchased and the time that the Event Table is created and available for use.

Invention

1. When transmitting an MPEG stream using a broadcast or other transmission medium, transmit the Event Table along with the associated MPEG stream. This allows the receiver to have access to the Event Table without decrypting the MPEG stream.

2. Encrypt the Event Table itself prior to transmission, to protect it from unauthorized use.

Provisional Patent Application

Authors: Daniel Zenchelsky, Andy Goodman, David Platt

Background

Audio, video, and/or data can be broadcast as a digital transport stream. The headend is the system responsible for creating the transport stream. A receiver is a device that receives and displays (or uses) the transport stream.

The headend can encrypt the transport stream to protect from unauthorized viewing (or use) of the data stream. In that case, the receiver is capable of decrypting the transport stream prior to viewing (or using) it.

The encryption algorithm used to encrypt the transport stream is controlled by an encryption key. The key is necessary to decrypt the transport stream. The key can be changed on a regular basis to increase security. By changing it on a regular basis, there can be multiple keys required to decrypt the transport stream. The keys can then be encrypted and broadcast within the transport stream.

On a receiver, the transport reception module (TRM) is responsible for receiving the transport stream from the transmission medium.

On a receiver, the Conditional Access Module (CAM) is responsible for deciding whether or not to decrypt the stream, based on the services that the user has purchased. If the CAM allows the user to view/use the transport stream, it decrypts the keys and provides them to the Transport Decryption Module (TDM) for use in decrypting the transport stream.

On a receiver, the TDM is responsible for decrypting the transport stream. The TDM uses the keys provided by the CAM to decrypt the transport stream.

On a receiver, the display module is responsible for displaying the decrypted transport stream to the user.

Problem

It is useful to be able to record the transport stream in its encrypted form. However, current conditional access systems are subject to key replay attacks.

Example

Both user A and user B record the transport stream that contains a particular audio/video stream (e.g. a movie). User A purchases the service and the CAM in his receiver provides the keys for use in decrypting the transport stream. User A records the keys that

are provided by the CAM, and sends them to user B. User B is then able to decrypt the stream that he also recorded, using the keys provided by User A. User B is then able to view the audio/video stream without purchasing it.

Solution Requirements

Provide multiple layers of protection. If one layer is circumvented, the others remain intact.

Layer 1 - Prevent the keys from being recorded from the CAM. This can be done by never exposing the unencrypted keys to the user or any user programmable processor within the system, or storing it within any user accessible memory within the system. Further, the communication path between the CAM and the TDM can be encrypted.

Layer 2 - Prevent the keys from being played back into the TDM. This can be done by ensuring that the TDM will not accept the actual key to the TDM, but instead requires a key that is transformed in such a way that it is unique to a particular receiver. Likewise, the CAM must be designed to provide such a transformed key.

One factor in the effectiveness of this layer is the difficulty in transforming a key received from one receiver□s CAM into the key required by a second receiver□s TDM. The more difficult this is, the better the protection.

Layer 3 — Prevent the user from decrypting the transport stream without using the TDM. This can be done by never exposing the transport stream to the user. The transport stream must be encrypted a second time before passing it through any user accessible memory, or through any user programmable processor within the system. This can be further enhanced by providing an encryption mechanism that produces a different encrypted stream on different receivers.

Implementation

The implementation is based on existing encryption technology, used in a new and unique way.

Headend has
Global Secret Key
Headend Private Key
Receiver□s Transport Public Key
Receiver□s CAM Public Key

TRM has
Transport Private Key
Headend Public Key

TDM has
Transport Private Key
Headend Public Key

CAM has
CAM Private Key
Headend Public Key
Global Secret Key
CAM Secret Key

CAM to TRM/TDM Pairing Procedure

1. Headend generates a random secret : S
2. Headend cryptographically signs S using Headend Public Key : HPK(S)
3. Headend encrypts S,HPK(S) using Transport Public Key : TPK(S,HPK(S))
4. Headend encrypts S,HPK(S) using CAM Public Key : CPK(S,HPK(S))
5. Headend transmits TPK(S,HPK(S)) and CPK(S,HPK(S)) to TRM
6. TRM decrypts TPK(S,HPK(S)) using Transport Private Key : S,HPK(S)
7. TRM verifies signature of HPK(S) using Headend Public Key. If signature is invalid, the processing stops here.
8. TRM stores shared secret, S, for future use
9. TRM passes TPK(S,HPK(S) to TDM
10. TDM decrypts TPK(S,HPK(S)) using Transport Private Key : S,HPK(S)
11. TDM verifies signature of HPK(S) using Headend Public Key. If signature is invalid, the processing stops here.
12. TDM stores shared secret, S, for future use
13. TRM passes CPK(S,HPK(S)) to CAM
14. CAM decrypts CPK(S,HPK(S)) using CAM Private Key : S,HPK(S)
15. CAM verifies signature of HPK(S) using Headend Public Key. If signature is invalid, the processing stops here.
16. CAM stores shared secret, S, for future use

Transport Stream Recording Procedure

1. Headend generates an encryption key : K
2. Headend encrypts key using Global Secret Key : GSK(K)
3. Headend transmits GSK(K) to TRM
4. Headend encrypts transport stream using K : K(TS)
5. TRM sends GSK(K) to CAM
6. CAM generates Local Key by encrypting GSK(K) using CAM Secret Key : LK= CSK(GSK(K))
7. CAM encrypts LK using shared secret, S : S(LK)
8. CAM sends S(LK) to TRM
9. TRM decrypts S(LK) using shared secret, S : LK
10. Headend transmits K(TS) to TRM
11. TRM further encrypts K(TS) using LK : LK(K(TS))
12. TRM stores GSK(K) and LK(K(TS)) on a storage medium

Transport Stream Playback Procedure

1. TDM retrieves GSK(K) and LK(K(TS)) from storage medium
2. TDM sends GSK(K) to CAM
3. CAM generates Local Key by encrypting GSK(K) using CAM Secret Key : LK= CSK(GSK(K))
4. CAM decrypts GSK(K) using GSK : K
5. CAM encrypts K,LK using shared secret, S : S(K,LK)
6. CAM sends S(K,LK) to Transport
7. TDM decrypts S(K,LK) using shared secret, S : K,LK
8. TDM decrypts LK(K(TS)) using LK : K(TS)
9. TDM decrypts K(TS) using K : TS
10. TDM sends Transport Stream, TS, to display module

Downloading Movies to Lots of People

James Barton

Elements:

- A population of TiVo Receivers
- A network supporting multi-cast packet transport
- A central scheduling system
- A server containing content of interest

Scenario:

- TiVo service produces program guide info describing programs stored on the video server and distributes it to TiVo receivers

- Viewer chooses a program for "recording". Instead of scheduling a recording, receiver sends request for the program to the TiVo service.

- TiVo service collects all requests and forwards them to a scheduling system. For most requested program, scheduling systems asks server to reliably multicast the program over the network to all receivers requesting it.

- When delivery is finished, the scheduler chooses another program to multicast. The choice can simply be to send the currently most requested program. This won't be good, as less requested programs may never be sent ("denial of service"). Thus, the scheduler will weight each program by the time since it was requested, with a limiting time perhaps a few days. If the limit is reached, that program is next to send. If several programs in that state, first come, first sent. If the weighted desireablity of the program exceeds that of the most popular program, the weighted program is sent next instead. This guarantees that the program will eventually be sent in a timely manner.

- There is no requirement or need that this delivery occur in real time.

Permutations:

- Multiple programs may be delivered at once if sufficient resources are available. This is a simple extension to the above scheduling system.

- Multicast is not strictly required. In this case, the program

is sent separately to each receiver. In this case, resources will limit the number of parallel streams. Scheduling is based on a business model that might take into account such factors as: viewer pays a premimum for fast delivery, pays a discount for "whenever" delivery; content provider pays a premium for "fast" delivery, or gets a discount for "whenever" delivery.

- Movies may be encrypted for delivery.

-end-end-end-end-end-

TiVo Receiver to TiVo Receiver Interactions

J. M. Barton

1. Introduction

Currently, TiVo receivers communicate only with the TiVo Service Center, which provides program guide data, graphical resources (such as fonts, pictures, etc.), service information, and other forms of data that enable the receiver to operate independently of the service to satisfy viewer interests. This communication uses a secure distribution architecture to move data between the receivers and the service such that service data is protected as well as the viewer's privacy.

It would be highly desireable to have a mechanism for moving media and database elements between two TiVo receivers. For instance, a "portable" receiver might provide a smaller amount of disk storage in a battery-driven device. Before going on vacation, the viewer might transfer desireable media (and, invisibly, associated service data) to the portable receiver, and take the portable receiver along, such that the media might be used when desired.

There are other receiver interactions that are also highly interesting, but transfer only control information of some kind. For instance, it might be desireable to slave two recievers together, such that two media streams are played with precise synchonization.

"Synchronizing" two receivers, such that resources, software and media streams are transferred between the two to achieve identical operation are also of interest.

2. Transferring Media Streams

A TiVo stored media stream really consists of two pieces: the content itself, and a database object which gives descriptive information about the content.

There are many ways in which to connect two TiVo receivers. The simplest is to plug the output of the source into the input of the destination. While functional, this method fails to transfer information about the media stream, which is essential to viewer satisfaction in managing and using the media stream.

If a data transfer method is used, such as a network (e.g., IEEE 802.3) or a direct connection (e.g., IEEE 1394), then both the content and the descriptive information can be transferred, such that the integrity of the viewer experience is preserved.

Content owners are concerned about theft of content. A further refinement of this method is to encrypt the data transfer between the receivers. This can be done in a number of standard and custom ways. For instance, the Diffie-Hellman secure connection protocol might be used to encrypt the transfer using a one-time key.

If it were desireable to allow the transfer to only occur to certain specified receivers, the integrated security system might be used. The public key of each receiver must be known to the other. When the transfer is started, the receivers exchange signed, encrypted certificates based on the stored private key. If both receivers can decrypt and verify the signature of the other, a one-time session key is then used to encrypt the data during the transfer.

Key distribution in such a case might be handled through the TiVo Service. A viewer would contact the service, and request that two receivers he owns be authorized for data transfer between each other. The service center would send a authorization object containing each receiver's public key to the other receiver through whatever download mechanism is appropriate. The TiVo service could maintain a record of this operation for later auditing purposes, which would include identifying information for each receiver.

For instance, should the security system be defeated in the receiver and the public key of the other be exposed, it might be possible to modify other receivers such that they appear authorized to the source receiver. Each receiver might keep a record of transfers which is uploaded to the service center. Later, this information could be processed to look for copy protection violations, copies to unauthorized receivers, etc.

If the transfer is interrupted, the destination reciever marks the media stream as "partial" in the descriptive object, much as is done today. Later, the transfer might be restarted. Since the design of the database system guarantees the media stream can be uniquely identified on the target device, the partial stream is found, and the transfer begins from it's end, thus avoiding re-transfer of media that has already been stored. Once all the stream is stored, the descriptive object is updated to show a complete media stream.

3. Download Speed

There is no particular real-time requirement necessary when transferring digital data between the receivers. Thus, the transfer might take place at whatever speed is appropriate. For instance, it may be the case that the network between the receivers is slow, in which case the transfer

duration will be longer than the playback duration of the content.

Alternatively, the network may be fast, in which case multiple media streams might be transferred in much less time than taken for playback of one content item. As happens today, the viewer on the target system may start viewing the media stream as soon as the first portions are available, in parallel with the ongoing download of the stream.

4. Other Types of Transfers

There is no requirement that the source or destination system be a complete TiVo receiver. For instance, it may be the case that media streams are stored on a server in a cable head end. The same mechanism described here can be used to transfer the content and descriptive information reliably to the destination receiver.

Alternatively, the desintation system might be the same head-end server, and the TiVo receiver performs a transfer to it.

5. Pre-Encrypted Media Streams

Certain media distribution architectures, such as digital satellite systems, broadcast most content in an encrypted state. Using a local decryption facility based on a smart-card, the media is decrypted only if viewed, thus protecting the content from theft.

It is possible for the TiVo receiver to save these encrypted media streams to disk, and to initiate decryption upon playback. It is also possible to use the methods described here to transfer media between two TiVo receivers. In order to properly obey a particular set of content protection rules associated with the media stream (such as play once, expire after 1 day, etc.), the current TiVo receiver maintains with the database object describing the media stream the copy protection information associated with the stream (including whether the stream is stored encrypted).

It is possible to transfer these same rules to the destination TiVo receiver. For example, the receiver may have stored a movie from a distribution service that will not be decrypted until viewed. If the viewer wishes to have this media stream transferred, it is simply copied into the media region of the destination TiVo, and the descriptive object transferred as well. This means that all original information on the stream is faithfully duplicated to the destination receiver.

The smart-card might be pulled from the original receiver and installed in the second. When the content is viewed, the viewer is properly charged and all copy protection rules followed. The original media and descriptive information might, or might not, be removed.

For instance, in a "view-once" scheme, the originals are destroyed, whereas in a "charge-per-view" scheme, the would not.

6. Control Interactions

Using the same techniques as described earlier, a secure, or authenticated and secure, connection might be established between two or more receivers using a network, perhaps accessed using the internal modem.

This enables control interactions to take place. Some examples are:

- Synchronized playback. A viewer might control trick-play features on a particular media stream. Each key event is also passed to the slave receiver, which automatically performs the same action. For example, a presenter might give a live presentation using TiVo as a multimedia playback device. An audience at a remote location could watch the same presentation given in the same way at the same time. Alternatively, two viewers communicating through some other means, perhaps a phone, might interact, while one or the other controls the playback on both receivers of the same program. This could allow precise discussion of the program of interest. The means of communication might be a simple chat program overlayed on the display in which the participants type comments.

- Link passing. A viewer might indicate that a particular program be "linked" to the slave. This results in a message sent to the slave which causes it to schedule recording of that program. Alternately, the program might be "unlinked" as well. The message need contain only the program ID, assuming both receivers are in service.

- Sound or graphics effects. When the viewer takes an action, such as pressing a particular key sequence, the receiver might play a sound or present a graphic. It would pass that event to the slave receiver(s) which would reproduce that same sound or graphic. For instance, a child might add sounds to a program this way, which would be replicated for his friend on a remote receiver. Clearly, such communication would be multi-way.

7. Updates

It may be useful for receivers to be able to transfer other types of data as well. For example, consider a large "home" receiver and a smaller "portable" receiver. Interesting data, such as software, graphical elements, program guide data, etc., might be transferred between two receivers as well, using the well-understood methods described in the database patent and the security provisions described earlier.

For instance, the portable receiver might be "updated" by the home

receiver every time the two are connected. This update might include transferring and installing a software update as well. The portable receiver would transfer any operational information to be sent to the TiVo service to the home receiver, which would later transfer it to the TiVo service.

One can also contemplate "automatic" operation. In such a case, when two receivers are connected, a set of pre-configured actions takes place, such as updating program guide or software, and then media streams might be transferred as well. If the destination system is smaller, then not all media streams would fit. In this case, the viewer might explictly choose which streams to transfer. A more interesting case occurs if preference information is used to choose a subset of the available media of most interest to the viewer and transfer only those streams. Another case might be where media streams are transferred going from newest to oldest, stopping when no more will fit, or oldest to newest, which is less interesting. Another criteria might be whether the program was explicitly picked or chosen based on viewer preferences. Any program information stored in the descriptive object for the content might be used in the selection criteria, such as length, actors, rating, etc.

-end-end-end-end-end-

PTO/SB/10 (1-99)
Approved for use through 09/30/2000, OMB 0651-0031
Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT CLAIMING SMALL ENTITY STATUS (37 CFR 1.9(f) & 1.27(c)) - SMALL BUSINESS CONCERN	Docket Number (Optional) TIVO0042

Applicant, Patentee, or Identifier: Barton et al.
Application or Patent No.:
Filed or Issued: Herewith
Title: Encryption System

I hereby state that I am
- [X] the owner of the small business concern identified below
- [ ] an official of the small business concern empowered to act on behalf of the concern identified below:

NAME OF SMALL BUSINESS CONCERN TiVo Inc.

ADDRESS OF SMALL BUSINESS CONCERN 894 Ross Drive, Sunnyvale, CA 94089

I hereby state that the above identified small business concern qualifies as a small business concern as defined in 13 CFR Part 121 for purposes of paying reduced fees to the United States Patent and Trademark Office. Questions related to size standards for a small business concern may be directed to: Small Business Administration, Size Standards Staff, 409 Third Street, SW, Washington, DC 20416.

I hereby state that rights under contract or law have been conveyed to and remain with the small business concern identified above with regard to the invention described in:

- [X] the specification filed herewith with title as listed above.
- [ ] the application identified above.
- [ ] the patent identified above.

If the rights held by the above identified small business concern are not exclusive, each individual, concern, or organization having rights in the invention must file separate statements as to their status as small entities, and no rights to the invention are held by any person, other than the inventor, who would not qualify as an independent inventor under 37 CFR 1.9(c) if that person made the invention, or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d), or a nonprofit organization under 37 CFR 1.9(e).

Each person, concern, or organization having any rights in the invention is listed below
- [ ] no such person, concern, or organization exists.
- [X] each such person, concern, or organization is listed below

Separate statements are required from each named person, concern or organization having rights to the invention stating their status as small entities. (37 CFR 1.27).

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b))

NAME OF PERSON SIGNING James M. Barton

TITLE OF PERSON IF OTHER THAN OWNER Sr. Vice President

ADDRESS OF PERSON SIGNING 894 Ross Drive, Sunnyvale, CA 94089

SIGNATURE _____ DATE Nov. 1, 2000

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231